Efficient and User Friendly Inter-domain Device Authentication/Access control for Home Networks

Jin-Bum Hwang, Hyung-Kyu Lee, and Jong-Wook Han

University of Science & Technology, Korea
Electronics and Telecommunications Research Institute, Korea
161 Gajeong-dong, Yuseong-gu, 305-350, Korea

{hjb64253, leehk, hanjw}@etri.re.kr

Abstract. Device authentication can reinforce the security of the home network services by ensuring that only specific authorized devices by specific authorized users can access the services. And it is also a mandatory technology for context-aware services in which users are not participant in the service flow. In this paper, we propose a device authentication and access control scheme based on two-layered PKI approach for efficient communication and user convenience. The two layers of our model are Global PKI layer and Localized PKI layer. Global PKI layer use conventional PKI model. There are only one global root CA and certificate verification is performed by validating the certificate-chain linked to the root CA. Otherwise, in Localized PKI layer, each home gateway take a role of root CA which is responsible for issuing device certificates to the devices belong to its domain. We use Global PKI layer for device registration and authentication of inter-home-network, but use Localized PKI layer to authenticate each end-device. Based on this separating, our model provides secure, efficient and user friendly multi-domain device authentication protocols. Based on this authentication, we also provide a convenient access control scheme using Attribute Mapping Certificate.

1 Introduction

The home network is an emerging technology which provides residents more comfortable and convenient living environment. Home networks consist of many networked devices and the devices provide users variable services such as home automation, data sharing, and context-aware service. Security in home networks is a more important problem than in traditional network environment, because the services provided in home networks is very closely related with the resident's privacy and safety (e.g. door lock/unlock, gas valve control, and remote healthcare) and compromising of the services can result in vast damages to the residents' property and body directly. Therefore, the security in home networks needs to be considered more carefully.

Authentication is a fundamental security mechanism that verifies principal's claimed identity. Generally, user authentication process verifies a user identity

through variable means such as password, identity certificate, smart cards, or biometrics. However, these user authentication mechanisms are prone to be easily compromised due to their intrinsic vulnerabilities or the users' inattention. Device authentication is one way that can complement these weaknesses. Device authentication ensures that only specific authorized devices by specific authorized users can access the services. This means that even if password or other user credential is compromised, the security between two parties is still protected as long as the authorized device is not used. Besides this, the device authentication is a mandatory technology that enables emerging context-aware services providing service automatically through device cooperation without user intervention, and DRM systems also need the device authentication [1,2].

So far, several mechanisms have been proposed for this purpose. Some industries suggest hardware fingerprint based approach [3,4] that extract the secret information from the unique hardware fingerprint and trust the device by verifying the secret. Bluetooth [5] and Zigbee [6] provide device authentication mechanism based on shared symmetric key, and CableLab [7] also provides PKI based one. Personal CA [8] and UPnP [9,10] provides localized PKI model. However, to the best of our knowledge none of them are applicable for multi-domain environment; they are not scaleable and not user friendly in multi-domain environment for several reasons [11].

In our previous work [11], we proposed a two-layered PKI model for device authentication in multi-domain home networks to solve existing problems, but it lacks relating the authentication scheme to an access control scheme. In this paper, we suggest a device authentication and access control mechanism based on the two-layered PKI model.

The rest of this paper is organized as follows. In Section 2 we explain the architecture of the two-layered PKI model for device authentication in multi-domain home networks. Next in Section 3, we describe our design of multi-domain device authentication model, and we show our device access control model in Section 4. Then we conclude and discuss our future work In Section 5.

2 Architecture of two layered PKI model

We present two layered PKI model, which consist of Global PKI layer and Localized PKI layer, for device authentication applicable to multi-domain home network environment. Fig 1 shows the architecture of our model.

The main principal of our architecture and protocol design is minimizing the end-device's operations, user intervention, and communication time delay in overall device authentication procedure for user friendly, efficient, and scalable device authentication. Generally, home gateways have uniform and more powerful computational capabilities than generic home devices, and they are always on, connected to Internet, and deployed only one at a home domain. These characteristics of the home gateway make it feasible to use the conventional PKI model in authentication process between them. In proposed model, Global root CA issues X.509 certificates to home gateways and manufacturer server, and conventional PKI

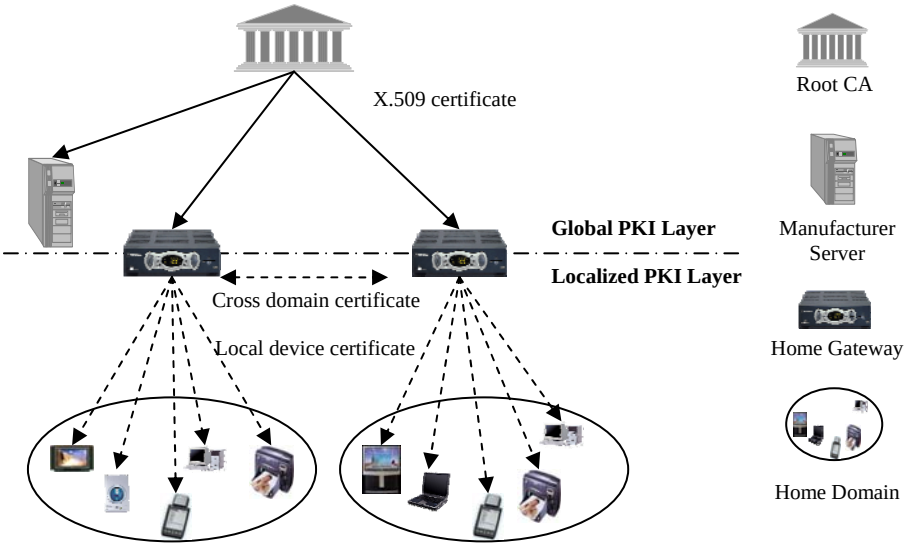

Fig. 1. Proposed device authentication model is consists of Global and Localized PKI Layer. The root CA issues X.509 certificate to Home gateway and Manufacturer Server (Subordinated CAs are omitted to simplify the figure.) Home gateway or Manufacture Server uses this certificate to authenticate each other in proposed protocols. The Home gateway has a role of CA in home domain and it issues a newly defined local device certificate to each home device.

management protocols are work among them. We named this conventional PKI layer as "Global PKI layer" against "Localized PKI Layer." Global PKI layer is responsible for authentication between manufacturer server and a home gateway during device registration process and authentication among home gateways during domain association process which will be described later.

Contrary to the home gateway, end-devices have variable characteristics according to their functions and many of them have limited capabilities in computational power and memory, although some devices, such as PC and media servers, have powerful computational power and large memory. In addition to this, the large number of deployed end-devices is a big obstacle to use the conventional PKI model in authentication of the devices due to the several reasons mentioned in Section 2. Therefore, we suggest localized PKI model for end-devices and provide safe, efficient and user friendly authentication protocols. This is Localized PKI layer. Two characteristics, always on and connected to Internet, enable the home gateway to have a role of root CA in this layer. The home gateway is responsible for issuing and managing local device certificates for end-devices and cross-domain certificate for other home gateways in Localized PKI layer. The cross-domain certificate makes the communication time delay optimized by eliminating the need of inter-domain communications. Table 1 shows the main fields of local device certificates.

Table 1. Main Fields of local device certificate

Field name	Description
Issuer	Issuer name of this certificate
Issuer public key	The public key of issuer
Subject	Subject name of this certificate. The name is unique in the local domain.
Subject public key	The public key of subject
Temper resistance level (for access control)	The device's temper resistance level. 1. Perfectly temper resistant 2. Hard to temper 3. Has some temper resistance function 4. Not temper resistant
Lost prevention level (for access control)	The jeopardy level of device loss or theft. 1. Hard to lose or be stolen 2. Possible to lose or be stolen 3. Easy to lose or be stolen
Domain name	The name of the domain to which this subject belongs
Domain URL	The URL of the Domain
Validate	The expiration date of this certificate

Finally, the manufacturer server is responsible for storing and providing device related information to the home gateway one of whose domain resident purchase the device. The information includes device security level and device public key information. The manufacturer server also acts as a trusted third party between the device and the home gateway during device registration process.

The details of the protocols will be described in next section.

3 Device Authentication

In this section, we illustrate proposed device authentication based on our two layered PKI architecture. Table 2 shows the notations we will use.

3.1 Device registration

Device registration is a mutual authentication process between a device and a home gateway for imprinting device and issuing local device certificate to the device. The device sets the home gateway's public key as the root public key after authenticate it and the home gateway issues a local device certificate to the device also after authenticate its identity.

Table 2. Notations for proposed protocols

Symbol	Denotation
$Gcert_X$	A X.509 certificate that the global CA issues to X.
$Ccert_{XY}$	A cross domain certificate that domain X issues to domain Y
$Lcert_{XY}$	A local device certificate that a home gateway X issues to Y
N_X	A nonce that X creates to prevent a replay attack.
K_{XY}	A symmetric key shared between X and Y
K_X	A public key of X
$( )K_{XY}$	An encryption using symmetric key K_{XY}
$( )K_X$	An encryption using X's public key
$( )K_{X^{-1}}$	A signature using X's private key
M	Manufacturer Server
D	A device
H	A home gateway
C	A client device
S	A service device
H_X	A home gateway to which X belongs

We use the manufacturer as a trusted third party in this process. The manufacturer has two well fitted features for this role. First, it can easily embed a secret shared between a device and itself to the device at manufacturing time, and also easily contact a user through out of band or authenticated channel to inform a $SecretID$ of the device when the user purchases the device. This characteristic makes the device registration more simple and user friendly. Through the manufacturer server, the user is only responsible for entering $SecretID$ received from the manufacturer in overall device registration process. Second, the manufacturer has qualification to certify the device's security characteristics. For example, it knows the device's temper resistance level and jeopardy level of lost or theft because it produces the device. This information can be used for device access control which will be described later.

We use the manufacturer as a trusted third party in this process. The manufacturer has two well fitted features for this role. First, it can easily embed a secret shared between a device and itself to the device at manufacturing time, and also easily contact a user through out of band or authenticated channel to inform a $SecretID$ of the device when the user purchases the device. This characteristic makes the device registration more simple and user friendly. Through the manufacturer server, the user is only responsible for entering $SecretID$ received from the manufacturer in overall

device registration process. Second, the manufacturer has qualification to certify the device's security characteristics. For example, it knows the device's temper resistance level and jeopardy level of lost or theft because it produces the device. This information can be used for device access control which will be described later.

Now, we describe the device registration protocol. The purposes of this protocol are securely transferring the root public key to a device and issuing local device certificate of Localized PKI layer to the appropriate device. For these purposes, the manufacturer server mediates the device and the home gateway to authenticate each other. Table 3 shows the device registration protocol and the detailed description can be found in [11].

Table 3. Device registration protocol

From → To	Message
1: $D \rightarrow H$	*Registration request*
2: $H \rightarrow D$	N_H
3: $D \rightarrow H$	$(D_{ID}, N_D, N_H)K_{MD}$
4: $H \rightarrow M$	$(D_{ID}, N_D, N_H)K_{MD}, (N_H, N_D, SecretID)K_{H^{-1}}, Gcert_H$
5: $M \rightarrow H$	$(K_H, N_D)K_{MD}, DevInfo, (N_H, DevInfo)K_{M^{-1}}, Gcert_M$
6: $H \rightarrow D$	$(K_H, N_D)K_{MD}, Lcert_{HD}$

In the case of authentication between the devices that belong to different domains, there are two states according to the relation between the two domains each device belongs to; "*Association Unestablished*" and "*Association Established*" *Association Unestablished* state is the one that the two domains have no security related information about each other. In this state, a device can't authenticate other domain's device. On the other hand, *Association Established* state is the one in which the two domains have a security association, and one domain's device can authenticate another domain's device based on this association. Two domains in *Association Unestablished* state can move to *Association established* state by issuing cross certificates each other and storing the domain name and public key. When a device requests a service to other device which belongs to different domain and the two domains are in *Association Unestablished*, the protocol, which establishes security association between two domains, is executed. We called this protocol "Inter-domain association protocol." Table 4 shows the messages exchanged in this protocol.

At first, the client requests authentication to the service domain home gateway with Nonce N_C and its local certificate. Then, the home gateway confirms whether it and the client domain home gateway are in *Association Established* state or not. If they are not, the service domain home gateway sends its global certificate to the client domain home gateway. Then, the client domain home gateway verifies the certificate, and if it is valid, issues cross domain certificate to the service domain home gateway and sends its global certificate together. Upon the receiving the certificate, the service

domain home gateway verifies the certificate and stores the client domain home gateway's domain name and public key.

Table 4. Inter-domain association protocol

From → To	Message
1: $C \rightarrow H_S$	$N_C, Lcert_{H_C C}$
2: $H_S \rightarrow H_C$	$Gcert_{H_S}$
3: $H_C \rightarrow H_S$	$Gcert_{H_C}, Ccert_{H_C H_S}$

Once the two domains enters into *Relation established* state, two devices belongs to each domain can authenticate each other without Global PKI layer until the cross domain certificates are revoked. This is "Inter-domain device authentication protocol" and table 5 shows the flow of this protocol.

At first, the client requests authentication to the service domain home gateway with Nonce N_C and its local certificate. Then, the home gateway confirms whether it and the client domain home gateway are in *Association Established* state or not. If they are, the service domain home gateway verifies the client's local certificate using the client domain home gateway's public key stored during the Inter-domain association protocol, and sends the cross domain certificate, signed message with its private key, and Attribute Mapping Certificate ($AttMappingCert$). Attributed Mapping Certificate will be described in next section. Then, the client device verifies the cross domain certificate and the signature of messages.

Table 5. Inter-domain device authentication protocol

From → To	Message
1: $C \rightarrow H_S$	$N_C, Lcert_{H_C C}$
2: $H_S \rightarrow C$	$Ccert_{H_C H_S}, (N_C)K_{H_S^{-1}}, AttMappingCert$

4 Device Access control

Access control is a process that decides whether grant or deny a request to access a specific service. After authenticating the client device, service domain's home gateway can know about the following client's information.

- *Device name*
- *Device's domain name*
- *Temper resistance level*
- *Lost prevention level*

The service device administrator can decide whether permit or deny the access to the device's service based on the confidence of the client device's domain. For example, if the domain is same with the one the service device belongs to, the client device can be granted access to most of the services. On the other hands, if the domain is a neighbor, the client device can access to limited services but it can access more services than unknown domain's device. The device name makes the decision more specific. The administrator can add or remove access authorities of the device according to the device's name. Although two devices are from same domain, one device can use more services than those permitted to the domain, but another can use fewer services than those according to the specific policies for the devices.

Device's temper resistance level and lost prevention level provide information how credible the device is. The secret such as private key can be easily compromised by physical attack if temper resistance technologies are not provided. The temper resistance level means that how well the device can resist against the physical attack to compromise the device's secret. Although the device's domain and the device itself are confident, the low temper resistant level device must not totally be trusted because it may be an adversary who already compromised the device's secret and impersonate the device. The lost prevention level is also important because the user of the device may be an adversary who stole the device from the owner. The low lost prevention level means that the device is likely to be stolen easily. So, the administrator should forbid the access to the critical services from low lost prevention level devices.

For this access control, we use two kinds of Attribute Mapping Certificates. Figure 2 shows the certificate issuing from a home gateway to end-devices.

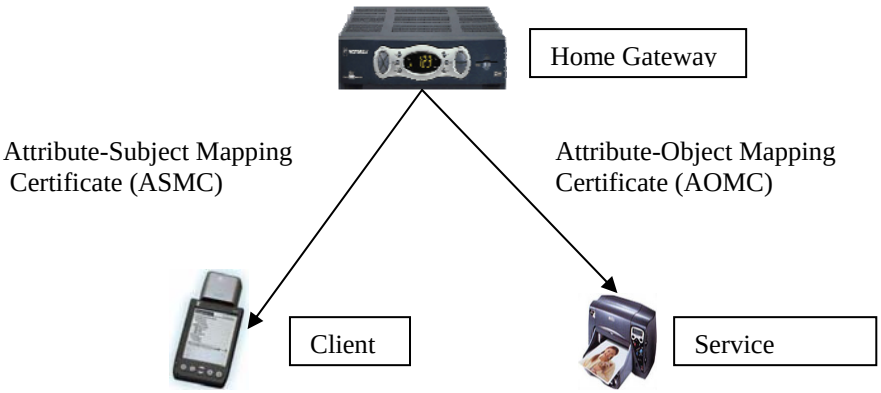

Fig. 2. The domain's Home gateway issues Attribute-Object Mapping to its domain's service devices and issues Attribute-Subject Mapping Certificate to a client.

At the first, the service domain's home gateway issues the AOMC to its domain's service devices. And upon receiving the request, the home gateway issues an ASMC to the client after authentication according to its access control policy for the client. The elements of these two certificates are shown in the figure 3.

The role of these certificates is that enforce the service devices to provide its service to the client who have the attributed described in the certificate. For example, a client who has an ASMC in which gold and silver attributes are described, it can use the services provided by the service devices who have the AOMC in which gold or silver attributes is described.

ObjectID	
Attribute1	Permissions
:	:
AttributeN	Permissions
Validity	
Signature	

a) Attribute-Object Mapping Certificate (AOMC)

SubjectPublicKey
Attribute1
:
AttributeN
Validity
Signature

b) Attribute-Subject Mapping Certificate (ASMC)

Fig. 3. ObjectID in AOMC is the service device identifier who is issued this certificate. AOMC can include several attributes and permissions allowed to the attribute. Validity is the expiration date of this certificate. SubjectPublicKey in ASMC is the client's public key. ASMC can have several attributes.

The access control protocol is as follows;

1. Client requests a service to a service device.
2. Service sends a nonce to the client and request to present its certificates.
3. Client signs the request message using it private key and send this message with its ASMC.
4. Service device verify the signature of the ASMC using its domain home gateway's public key. Then, if the certificate is valid and it includes a required attribute, the service device provides requested service to the client.

With the Attribute-Mapping Certificate the client can use all of the domain's service authorized to it without the authentication on the domain's home gateway. And the service can authorize the client without the detail information about client and the home gateways help. This can simplify the management of the access control policy.

5 Conclusions

We have suggested a device authentication and access control model for multi-domain home network environments. The main goals of our architecture and protocol design are minimizing the end-device's operations, user interventions, and communication time delay in over all device authentication and access control process. For these purposes, our model uses two layered PKI approach for scalable, efficient, and user friendly device registration and authentication. Global PKI layer participate on the device registration protocol and inter-domain association protocol, and Localized PKI layer is in charge of the authentication between end-devices. The X.509 certificate, which Global PKI layer uses, enables user friendly device registration and inter-domain authentication, and the Local device certificate and the Cross domain certificate makes the end-device authentication efficient and scalable in multi-domain environment. And the attribute mapping certificates makes the access control policy management of service devices simple and convenient. In our model, the device registered to one domain can be authenticated and authorized in other domains without other registration process, and the authentication and access control protocol between two end-devices executed only in local domain without inter-domain communications.

References

1. Yeonjeong Jeong, Kisong Yoon, and Jaesheol Ryou, A Trusted Key Management Scheme for Digital Rights Management, ETRI Journal, vol.27, no.1, Feb. 2005, pp.114-117.
2. Junseok Lee, et al., A DRM Framework for Distributing Digital Contents through the Internet, ETRI Journal, vol.25, no.6, Dec. 2003, pp.423-436.
3. Device Authentication. http://www.safenet-inc.com
4. TrustConnector 2. http://www.phoenix.com
5. Bluetooth Core Specification v2.0. http://www.bluetooth.org/spec/, 2004
6. ZigBee Specification v1.0, December 2004, http://www.zigbee.org/en/spec_download/
7. OpenCable Security Specification. http://www.opencable.com/specifications/, 2004
8. Gehrmann, C., Nyberg, K., and Mitchell, C.J.: The personal CA - PKI for a personal area network. [Conference Paper] IST Mobile and Wireless Telecommunications Summit 2002, pp.31-5, 2002.
9. Universal Plug and Play Forum, http://www.upnp.org/
10. Ellison, C.: UPnP Security Ceremonies Version 1.0. UPnP Forum, 2003.
11. Jin-Bum Hwang, Do-Woo Kim, Yun-Kyung Lee and Jong-Wook Han, Two Layered PKI Model for Device Authentication in Multi-Domain Home Networks, Proc. of 10th International Symposium on Consumer Electronics (ICSE), June 2006